“Implementación de Seguridad Perimetral en Entornos GNU/Linux mediante Endian Firewall y Servicios de Red en Infraestructura Virtualizada “

Alvaro Enrique Mejia
e-mail: aemejia@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de un entorno seguro en GNU/Linux utilizando la distribución Endian Firewall Community como plataforma central de seguridad perimetral. Se desarrolló un laboratorio virtualizado en Oracle VirtualBox, configurando una red segmentada en tres zonas lógicas: Zona Verde (LAN), Zona Roja (WAN) y Zona Naranja (DMZ). En la primera etapa, se instaló y configuró Endian asignando interfaces de red específicas para cada zona, asegurando la conectividad interna y hacia Internet simulada.*

Posteriormente, se aplicaron reglas de NAT (Network Address Translation) para permitir la salida controlada del tráfico desde la LAN y la DMZ hacia la WAN. En la DMZ se implementaron servicios web (HTTP) y FTP sobre un servidor Ubuntu Server, configurando reglas de firewall que permiten o bloquean el acceso a estos servicios según el origen y destino del tráfico. Además, se bloqueó el protocolo ICMP para evitar diagnósticos de red no autorizados.

Se definieron reglas interzonales para regular el tráfico HTTP y FTP entre LAN, DMZ e Internet, incluyendo validaciones desde navegadores y herramientas de línea de comandos. Finalmente, se configuró un proxy HTTP no transparente con políticas de autenticación y filtrado de contenidos, bloqueando el acceso a sitios específicos mediante una lista negra personalizada.

La solución implementada demuestra el uso práctico de herramientas de código abierto para diseñar e implementar un sistema de seguridad perimetral robusto, que protege los servicios críticos y regula el acceso a los recursos en un entorno de red controlado y replicable.

PALABRAS CLAVE: Endian Firewall, Seguridad perimetral, Proxy HTTP, DMZ, GNU/Linux

1 INTRODUCCIÓN

La creciente complejidad de los entornos de red en organizaciones modernas demanda mecanismos robustos de seguridad perimetral que permitan controlar, monitorear y restringir el tráfico entre diferentes zonas lógicas de red. En este contexto, la segmentación mediante zonas como LAN (Zona Verde), WAN (Zona Roja) y DMZ (Zona Naranja) se convierte en una estrategia clave para proteger los recursos críticos y minimizar los riesgos de accesos no autorizados.

Este artículo presenta el desarrollo de una infraestructura de red virtualizada con herramientas de código abierto, utilizando Endian Firewall Community 3.3.2 como elemento central de control de tráfico. La solución se implementó en VirtualBox, asignando interfaces de red específicas a cada zona y desplegando un servidor Ubuntu en la DMZ para ofrecer servicios HTTP y FTP.

A lo largo del proyecto, se configuraron reglas de NAT (Network Address Translation) para permitir la salida segura desde la LAN y la DMZ hacia Internet simulada, así como políticas de firewall para permitir o denegar servicios según su origen y destino. Además, se integró un proxy HTTP no transparente con autenticación de usuarios y filtrado web, reforzando las políticas de navegación segura desde la LAN.

El desarrollo de este entorno no solo permitió aplicar conceptos teóricos de seguridad de redes, sino también fortalecer competencias técnicas en la administración de sistemas GNU/Linux, el uso de firewalls perimetrales y la gestión de servicios esenciales bajo criterios de aislamiento, autenticación y control de tráfico.

2 FORMATO

2.1 CARACTERÍSTICAS GENERALES

Endian Firewall Community (EFW) es una distribución basada en Linux diseñada específicamente para servir como una solución de seguridad perimetral todo-en-uno. Se caracteriza por ofrecer un enfoque modular y centralizado para la gestión de redes seguras, incorporando funcionalidades como firewall con inspección de paquetes, NAT, VPN, filtrado web, servidor proxy y sistema de detección de intrusos (IDS). Esta arquitectura se representa en la Figura 1.

Una de las ventajas más destacadas de EFW es su interfaz web intuitiva, que permite al administrador configurar reglas, monitorear tráfico y gestionar servicios sin necesidad de conocimientos avanzados en línea de comandos. Además, EFW se encuentra disponible en versión comunitaria y empresarial, siendo la comunitaria de código abierto y gratuita, ideal para ambientes académicos o de pequeña empresa.

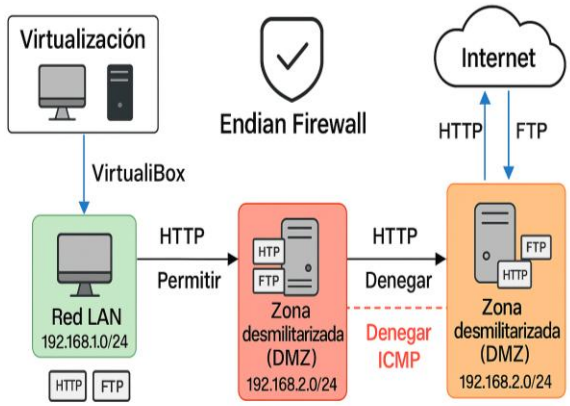
Sus principales características técnicas incluyen:

- Soporte para zonas de seguridad diferenciadas: Verde (LAN), Roja (WAN), Naranja (DMZ) y Azul (WLAN).

- Administración de servicios como DHCP, DNS, VPN (IPSec y OpenVPN) y NAT.
- Sistema de proxy HTTP con autenticación y listas de control de acceso.
- Registros detallados (logs) de tráfico y eventos, integrados en el panel de control.

- Compatibilidad con entornos virtualizados como VirtualBox, VMware y KVM.

Figura 1. Implementación de seguridad perimetral con Endian Firewall en un entorno virtualizado usando GNU/Linux.



Fuente: Elaboración propia.

Estas características hacen de Endian una herramienta poderosa para implementar esquemas de seguridad robustos, centralizados y adaptables a distintos niveles de complejidad organizacional.

3 TÍTULO PRINCIPAL

IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE SEGMENTACIÓN DE REDES Y CONTROL DE TRÁFICO CON ENDIAN FIREWALL EN ENTORNO VIRTUALIZADO

4 NOMBRES DE LOS INTEGRANTES Y SUS E-MAIL

Integrante Alvaro Enrique Mejia
e-mail: aemejia@unadvirtual.edu.co

5 SEGUNDA Y PÁGINAS SIGUIENTES

5.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

La implementación de una solución de seguridad perimetral inicia con la configuración adecuada del entorno virtual. En esta etapa se procedió a instalar la distribución Endian Firewall Community 3.3.2 en VirtualBox, y se configuraron tres interfaces de red que representan las zonas clásicas en una arquitectura de firewall: verde (LAN), roja (WAN) y naranja (DMZ).

Cada zona fue enlazada a un tipo de adaptador virtual diferente, lo cual permitió simular un entorno corporativo con salida a Internet, red local interna y una zona desmilitarizada para exposición controlada de servicios.

5.1.2 Configuración de la máquina virtual

Se creó una máquina virtual en Oracle VirtualBox con los siguientes parámetros:

Sistema operativo: Linux 64-bit

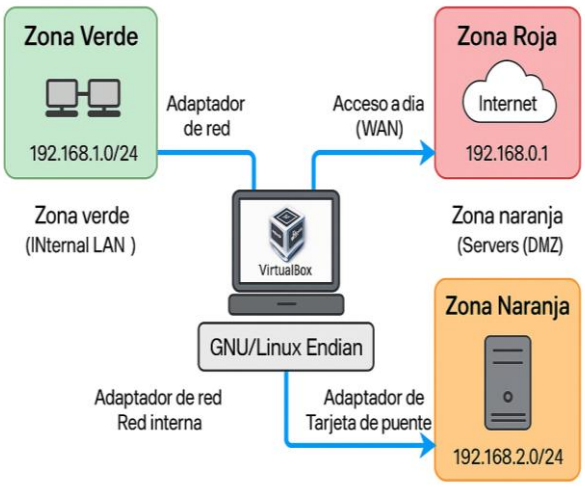
Memoria RAM asignada: 2048 MB

Disco duro: 40 GB VDI (almacenamiento dinámico)

ISO instalada: Endian Firewall Community 3.3.2

La topología de red utilizada se muestra en la Figura 2.

Figura 2. Topología de red propuesta con Endian Firewall.



Fuente: Elaboración propia.

5.1.3 Configuración de tarjetas de red

Se asignaron tres adaptadores de red a la máquina virtual, configurados de la siguiente manera:

Adaptador 1 (eth0): Modo NAT → asignado a la Zona Roja (WAN)

Adaptador 2 (eth1): Red interna → asignado a la Zona Verde (LAN)

Adaptador 3 (eth2): Adaptador solo-anfitrión → asignado a la Zona Naranja (DMZ)

Estas configuraciones permiten simular tráfico hacia Internet, comunicación interna entre equipos de la LAN, y exposición controlada de servicios públicos en la DMZ.

5.1.4 Instalación de Endian Firewall

Durante la instalación de Endian, se ejecutó el asistente de configuración de red:

- Zona Verde (br0) → 192.168.1.1/24
- Zona Naranja (br1) → 172.16.0.1/24
- Zona Roja (eth0) → 192.168.0.13/24

Se accedió a la consola web del firewall desde un navegador en la red LAN, a través de la URL https://192.168.1.1:10443, lo cual confirmó la disponibilidad de la interfaz de administración.

5.1.5 Validación de interfaces y conectividad

Desde la consola de Endian, se verificó el estado de las interfaces con: ip addr show

Se observó lo siguiente:

- br0 (Zona Verde): 192.168.1.1
- br1 (Zona Naranja): 172.16.0.1
- eth0 (Zona Roja): 192.168.0.13

Desde un cliente Ubuntu Desktop ubicado en la zona verde, se comprobó conectividad hacia el firewall (ping a 192.168.1.1) y hacia la DMZ (ping a 172.16.0.1), confirmando el enrutamiento y la correcta segmentación de red.

5.1.6 Resultado de la implementación

Se logró establecer la arquitectura segmentada con las siguientes características:

Zona	Tipo de Red	Dirección IP del Firewall
Verde (LAN)	Red Interna	192.168.1.1
Naranja (DMZ)	Solo anfitrión	172.16.0.1
Roja (WAN)	NAT (Internet simulada)	192.168.0.13

5.1.7 Aprendizajes adquiridos

Comprensión de la segmentación de redes perimetrales mediante zonas lógicas.

Configuración detallada de interfaces de red virtuales en VirtualBox.

Uso del firewall Endian para inicializar zonas y validar conectividad entre ellas.

Familiarización con herramientas de diagnóstico de red en GNU/Linux (ping, ip route, ip addr).

Esta base técnica es esencial para las temáticas posteriores que incluyen NAT, servicios en DMZ, políticas de acceso y proxy con autenticación.

5.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

La Traducción de Direcciones de Red (NAT) es una técnica fundamental en entornos de red que permite a dispositivos en redes privadas acceder a redes externas como Internet mediante una única dirección IP pública o de salida. En la implementación de seguridad perimetral con Endian Firewall, se configuraron reglas de NAT fuente (SNAT) para habilitar la comunicación saliente desde la zona Verde (LAN) y la zona Naranja (DMZ) hacia la zona Roja (WAN simulada), representando el acceso a Internet.

5.2.1 Objetivos técnicos

Configurar reglas SNAT para permitir tráfico saliente desde la LAN y DMZ hacia la WAN.

Verificar que los dispositivos en la LAN y DMZ puedan acceder a recursos externos simulados.

Validar visualmente la creación de las reglas en la interfaz gráfica del firewall.

Confirmar la funcionalidad de NAT mediante comandos de red.

5.2.2 Requisitos previos

Antes de aplicar las reglas de NAT, se deben cumplir las siguientes condiciones:

Interfaces correctamente asignadas en Endian:

- Zona Verde (br0): 192.168.1.1/24
- Zona Naranja (br1): 172.16.0.1/24
- Zona Roja (eth0): 192.168.0.13/24

Clientes funcionales en la zona LAN (Ubuntu Desktop) y un servidor en la DMZ (Ubuntu Server).

Acceso a la consola web de Endian en https://192.168.1.1:10443.

5.2.3 Configuración de reglas NAT

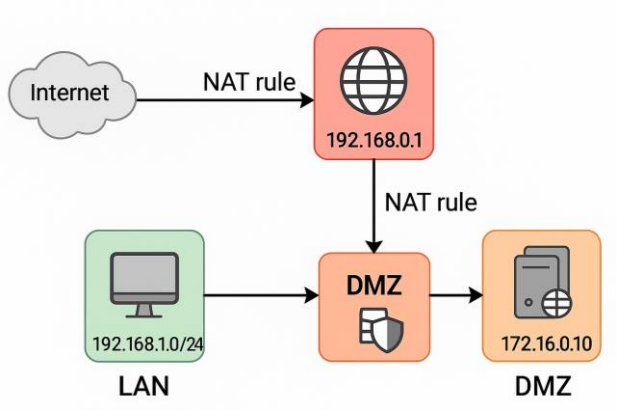
Las reglas fueron configuradas desde la interfaz web de Endian siguiendo estos pasos:

Regla NAT: LAN → WAN

Ruta de acceso: Firewall > NAT fuente
Origen: Zona Verde (LAN) 192.168.1.0/24
Destino: Zona Roja (WAN)

La configuración de esta regla se puede observar en la Figura 3.

Figura 3. Regla de NAT que permite salida desde la LAN hacia la WAN.



Fuente: Elaboración propia.

Tipo de NAT: Masquerading (enmascaramiento dinámico)

Estas reglas permiten que cualquier equipo de la LAN o DMZ utilice la IP de salida de la zona roja (192.168.0.13) como punto de traducción para acceder a servicios externos.

5.2.4 Verificación de la funcionalidad

Las siguientes pruebas se realizaron para validar el comportamiento de NAT en la infraestructura configurada:

5.2.5 Prueba desde estación LAN:

ping 8.8.8.8
curl http://example.com

Resultado: El servidor en la zona naranja logró comunicarse con la red externa simulada, lo cual valida la regla SNAT para la DMZ.

5.2.6 Revisión de reglas activas

Desde la interfaz web de Endian, se puede visualizar la lista de reglas de NAT aplicadas con su estado de activación. En caso de uso avanzado, se pueden listar mediante consola: iptables -t nat -L -n -v

5.2.7 Consideraciones sobre NAT y reenvío de puertos

En caso de necesitar acceso desde la WAN hacia la DMZ, es necesario implementar reglas de DNAT (Destination NAT) en el módulo NAT de destino de Endian, especificando los puertos a reenviar (por ejemplo, HTTP o FTP) al servidor de la DMZ. Aunque este artículo se centra en el acceso saliente (SNAT), estas configuraciones de DNAT son esenciales para servicios públicos como un sitio web expuesto externamente.

5.2.8 Diferencias entre SNAT y DNAT en el contexto de Endian Firewall

Endian Firewall permite aplicar dos tipos principales de traducción de direcciones IP: **SNAT (Source NAT)** y **DNAT (Destination NAT)**. Aunque ambas se implementan dentro del módulo de NAT del sistema, tienen funciones y propósitos distintos:

SNAT (Source NAT): Se utiliza cuando los dispositivos internos (LAN o DMZ) necesitan acceder a recursos externos, como Internet. Endian reemplaza la IP de origen del paquete por la IP de la interfaz de salida (por ejemplo, la de la zona roja), lo que permite que múltiples dispositivos naveguen hacia afuera utilizando una sola IP pública o simulada. Este mecanismo se aplica mediante la función de *masquerading* en el firewall.

DNAT (Destination NAT): Se emplea cuando es necesario **exponer un servicio interno** (como un servidor web en la DMZ) hacia el exterior. Endian intercepta una solicitud que llega desde la WAN a una IP o puerto específico y la redirige internamente hacia la dirección del servidor que realmente ofrecerá el servicio. Es útil, por ejemplo, para publicar servicios como HTTP o FTP al exterior de forma controlada.

Ambos tipos de NAT pueden coexistir y deben ser gestionados con precisión para evitar conflictos de reglas o aperturas innecesarias.

5.2.9 Conclusiones parciales

La implementación de reglas de NAT en Endian permitió establecer una política efectiva de salida controlada hacia redes externas desde segmentos internos. El uso de masquerading facilita el acceso a Internet sin exponer las direcciones IP internas, cumpliendo con principios de seguridad y eficiencia en la administración de tráfico. Estas configuraciones son fundamentales en esquemas de seguridad perimetral y representan una competencia clave en la administración de sistemas GNU/Linux.

5.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

En arquitecturas de seguridad perimetral, la zona desmilitarizada (DMZ) aloja servicios que requieren accesibilidad desde redes internas (LAN) y, en algunos casos, desde el exterior (WAN). Para mantener la seguridad del

entorno, estos servicios deben exponerse controladamente, mediante reglas específicas que permitan ciertos protocolos (como HTTP y FTP), y restrinjan otros que puedan facilitar la recolección de información, como ICMP.

Esta sección detalla cómo se habilitaron los servicios HTTP (puerto 80) y FTP (puerto 21) en un servidor Ubuntu Server ubicado en la zona naranja (DMZ), y cómo se bloqueó el protocolo ICMP (puertos 8 y 30), usando el firewall perimetral Endian.

5.3.1 Objetivos técnicos

Instalar y activar servicios web (Apache2) y FTP (vsftpd) en la DMZ.

Configurar el firewall de Endian para permitir tráfico HTTP y FTP entre zonas.

Bloquear solicitudes ICMP entrantes/salientes (ping).

Verificar el comportamiento desde terminales cliente (LAN) y el monitoreo de tráfico en Endian.

5.3.2 Configuración del servidor en la zona DMZ

El servidor ubicado en la DMZ (Ubuntu Server) fue preparado con los siguientes servicios esenciales:

Instalación de servidor web
sudo apt update
sudo apt install apache2 -y

Instalación de servidor FTP
sudo apt install vsftpd -y

Después de la instalación, ambos servicios fueron habilitados y verificados:

sudo systemctl enable apache2
sudo systemctl start apache2
sudo systemctl enable vsftpd
sudo systemctl start vsftpd

El servidor fue configurado con la IP 172.16.0.2, asignada estáticamente dentro del rango de la zona naranja.

5.3.3 Reglas de firewall en Endian

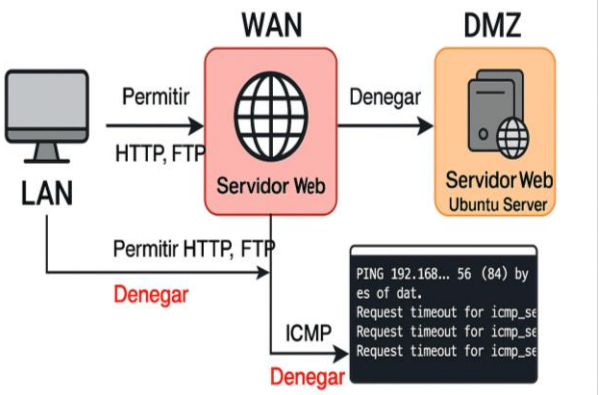
Permitir HTTP y FTP desde otras zonas hacia la DMZ

Desde la interfaz web de Endian, se crearon las siguientes reglas en: Ruta: Firewall > Reglas

Origen	Destino	Servicio	Acción
Zona Verde	Zona Naranja	HTTP (80)	Permitir
Zona Verde	Zona Naranja	FTP (21)	Permitir

Estas reglas habilitan el acceso desde clientes en la LAN hacia el servidor en DMZ para probar acceso a sitios web y transferencia de archivos.
La aplicación de estas reglas se ilustra en la Figura 4.

Figura 4. Permitir servicios de la zona DMZ para la red.



Fuente: Elaboración propia.

5.3.4 Verificación de servicios

Prueba desde cliente Ubuntu Desktop en LAN

Acceso a página web del servidor en DMZ
curl http://172.16.0.2

Conexión al servidor FTP
ftp 172.16.0.2

5.3.5 Resultado esperado:

El servidor Apache responde con contenido HTML predeterminado.

Se establece conexión al servidor FTP, solicitando autenticación.

5.3.6 Bloqueo de protocolo ICMP (Echo y Traceroute)

El protocolo ICMP es utilizado frecuentemente por herramientas como ping o traceroute para descubrir redes o equipos activos. Para evitar diagnósticos no autorizados, se bloquearon los tipos ICMP 8 (echo-request) y 30 (traceroute) desde la interfaz de Endian.

5.3.7 Reglas aplicadas - Ruta: Firewall > Reglas

Origen	Destino	Protocolo	Tipo ICMP	Acción
Cualquier zona	Cualquier zona	ICMP	Echo-request (8)	Denegar
Cualquier zona	Cualquier zona	ICMP	Traceroute (30)	Denegar

5.3.8 Alternativamente, también se puede hacer desde consola (modo experto):

iptables -A INPUT -p icmp --icmp-type 8 -j DROP
iptables -A INPUT -p icmp --icmp-type 30 -j DROP

5.3.9 Verificación de bloqueo ICMP

Desde un cliente en la LAN:
ping 172.16.0.2
traceroute 172.16.0.2

5.3.10 Resultado esperado:

El servidor en DMZ no responde a las solicitudes ICMP.
Traceroute no completa su recorrido.

5.3.11 Comprobación de tráfico en la interfaz de Endian

Desde la sección Logs > Firewall logs, se monitorearon las conexiones HTTP y FTP permitidas y los paquetes ICMP rechazados, lo cual confirma que las reglas están operando correctamente.

5.3.12 Conclusiones parciales

La habilitación controlada de servicios web y FTP en la zona DMZ permite ofrecer funcionalidades clave sin comprometer la seguridad de la red interna. La denegación de ICMP impide recolección de información sensible, como disponibilidad de equipos o topología de red. Esta configuración refuerza el principio de "mínimo privilegio", asegurando que solo el tráfico explícitamente permitido pueda cruzar las fronteras entre zonas.

5.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Una arquitectura de red segura no sólo se basa en la segmentación, sino en el establecimiento riguroso de reglas de acceso interzonales. Estas reglas deben definir explícitamente qué servicios están permitidos o denegados entre la Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja (WAN). Usar firewalls como Endian permite aplicar estos filtros con precisión, favoreciendo la reducción de superficie de ataque y asegurando un comportamiento predecible del tráfico.

5.4.1 Objetivos técnicos

Establecer reglas que permitan comunicación **HTTP (puerto 80)** y **FTP (puerto 21)** entre las zonas LAN y DMZ.

Configurar reglas que permitan el tráfico desde la zona Internet (WAN) hacia los servicios expuestos en la DMZ.

Validar el tráfico permitido en los logs del firewall.

Comprobar el funcionamiento de las reglas mediante navegadores web.

5.4.2 Reglas LAN (Verde) ↔ DMZ (Naranja)

Origen	Destino	Servicio	Acción
Zona Verde	Zona Naranja	HTTP (80)	Permitir
Zona Verde	Zona Naranja	FTP (21)	Permitir

5.4.3 Reglas DMZ (Naranja) ↔ WAN (Roja)

Origen	Destino	Servicio	Acción
Zona Naranja	Zona Roja	HTTP (80)	Permitir
Zona Naranja	Zona Roja	FTP (21)	Permitir

5.4.4 Verificación en tráfico interzonal

Para validar la efectividad de las reglas, se accedió a la sección **Logs > Firewall Logs** en Endian. Se observó:

- Paquetes permitidos con dirección origen/destino correctas.
- Protocolos coincidentes con las reglas configuradas.
- Confirmación de estado "ACCEPTED" en eventos relacionados con los servicios HTTP/FTP.

Además, en consola se puede ejecutar:

iptables -L FORWARD -v --line-numbers

Para verificar tráfico procesado por las reglas interzonales.

5.4.5 Pruebas desde navegador web

Se llevaron a cabo pruebas funcionales desde diferentes clientes ubicados en las zonas LAN, DMZ y WAN simulada:

Desde cliente en la zona verde (LAN):

- http://172.16.0.2 → Acceso HTTP al servidor en la DMZ (✓)
- ftp://172.16.0.2 → Acceso FTP a la DMZ (✓)
- http://192.168.0.1 → Acceso HTTP a la WAN (✓)
- ftp://192.168.0.1 → Acceso FTP a la WAN (✓)

Desde servidor en la zona naranja (DMZ):

- curl http://192.168.0.1 → Acceso a Internet simulado (✓)

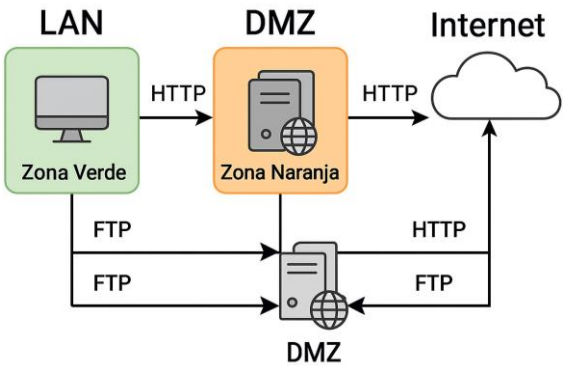
Desde cliente simulado en la zona roja (WAN):

- http://172.16.0.2 → Acceso web al servidor en DMZ (✓)

- ftp://172.16.0.2 → Acceso FTP al servidor en DMZ (✓)

Importante: En un entorno real, se recomienda no permitir tráfico WAN → DMZ sin autenticación o inspección profunda de paquetes, por razones de seguridad.
La Figura 5 resume las reglas de acceso configuradas entre las distintas zonas.

Figura 5. Tabla de reglas de tráfico permitidas y denegadas entre zonas.



Fuente: Elaboración propia.

5.4.6 Conclusiones parciales

La implementación de reglas interzonales específicas permitió comprobar la correcta segmentación y el control del tráfico. Se validó la conexión bidireccional controlada entre LAN y DMZ, así como entre DMZ y WAN, solo para los servicios requeridos. El firewall Endian facilita una administración detallada de políticas y la visualización de registros de tráfico en tiempo real, reforzando la trazabilidad y el cumplimiento del principio de mínimo privilegio.

5.5 TEMÁTICA 5: IMPLEMENTACIÓN DE UN PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

La integración de un servidor proxy en una red perimetral permite controlar y registrar el tráfico web, filtrar contenidos y establecer políticas de navegación. En entornos educativos o empresariales, es fundamental disponer de mecanismos que permitan no solo limitar el acceso a sitios web no deseados, sino también identificar al usuario responsable de cada conexión. Endian Firewall permite implementar un **proxy HTTP no transparente**, es decir, uno en el que el navegador debe estar explícitamente configurado para utilizarlo, lo que lo hace ideal para implementar autenticación de usuarios y control de contenido.

5.5.1 Objetivos técnicos

- Activar y configurar el **proxy HTTP no transparente** en Endian.
- Crear una lista negra personalizada para bloquear sitios específicos.
- Establecer un sistema de **autenticación por usuario** para controlar el acceso.
- Verificar que la política se aplique correctamente desde clientes en la zona LAN.

5.5.2 Configuración del Proxy HTTP en Endian

Activación del proxy no transparente
Desde la consola web de Endian:

- Navegar a: Servicios > Proxy HTTP
- Desmarcar la opción de “Proxy transparente”.
- Habilitar el proxy en el puerto 8080.
- Guardar los cambios.

En los navegadores de los clientes de la LAN (por ejemplo, Firefox o Chromium), se configuró manualmente la conexión al proxy con los siguientes datos:

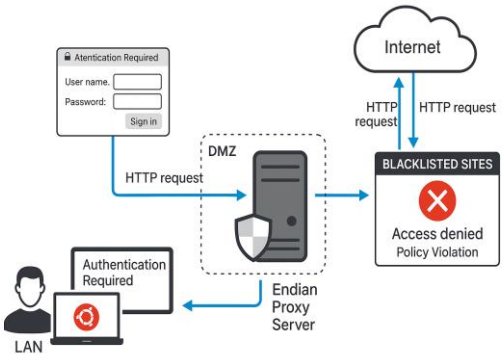
- **IP del proxy**: 192.168.1.1
- **Puerto**: 8080
- **Creación del perfil de filtrado (lista negra)**

Desde la interfaz de administración:

1. Navegar a Proxy HTTP > Filtro de contenido > Perfiles
2. Crear un nuevo perfil llamado bloqueo_web
3. En la sección de **lista negra**, agregar los siguientes dominios:
   - www.hotmail.com
   - www.youtube.com
   - www.elnuevodia.com.co
4. Activar el filtrado por lista negra y guardar el perfil.

Esta configuración se ejemplifica en la Figura 6.

Figura 6. Configuración del perfil de acceso y lista negra en el proxy HTTP de Endian.



Fuente: Elaboración propia.

5.5.3 Autenticación por usuario

Creación del usuario y grupo

1. Ir a Sistema > Administración de usuarios
2. Crear un nuevo usuario:
    - **Nombre de usuario**: usuario1
    - **Contraseña segura**: ********
3. Crear un grupo llamado grupo_proxy y asociar al usuario usuario1.

5.5.4 Vinculación del perfil al grupo

1. Ir a Proxy HTTP > Políticas de acceso
2. Crear una nueva política:
    - **Nombre**: control_por_usuario
    - **Usuarios o grupos permitidos**: grupo_proxy
    - **Perfil de filtrado aplicado**: bloqueo_web
    - **Método de autenticación**: Interno (usuarios de Endian)
3. Guardar y aplicar.

5.5.5 Pruebas desde la zona LAN

En el cliente Ubuntu Desktop en la zona verde (LAN):

1. Abrir navegador web.
2. Configurar proxy manual en 192.168.1.1:8080.
3. Al intentar acceder a los sitios bloqueados:
http://www.hotmail.com
http://www.youtube.com
http://www.elnuevodia.com.co

Resultado esperado: Aparece mensaje de "Acceso denegado por política de filtrado".

4. Al acceder a un sitio no bloqueado como http://www.wikipedia.org, la navegación es permitida.
5. Se solicita autenticación del usuario la primera vez, con credenciales de usuario1.

5.5.6 Registro de eventos y validación

En la sección Logs > Proxy HTTP, se pueden visualizar los siguientes eventos:

- Nombre de usuario que accedió.
- URL solicitada.
- Acción tomada: Permitido / Bloqueado.
- Hora y fecha del intento.

5.5.7 Conclusiones parciales

El uso de un **proxy HTTP no transparente** en Endian proporciona un control fino sobre la navegación en la red LAN. La posibilidad de aplicar filtros por usuario y registrar actividad fortalece la trazabilidad y la política institucional de navegación segura. La implementación de listas negras y autenticación interna es sencilla, pero robusta, y permite escalabilidad a escenarios más complejos (por ejemplo, integración con LDAP o Active Directory).

6 TEXTO PRINCIPAL

La presente implementación se desarrolló en un entorno virtualizado mediante VirtualBox, simulando una arquitectura de red empresarial con segmentación lógica y controles perimetrales de tráfico, basados en la distribución Endian Firewall Community y sistemas operativos GNU/Linux.

6.1 Infraestructura virtual y segmentación de red

Se desplegó una instancia de Endian configurada con tres interfaces de red virtuales:

Zona verde (LAN): red interna para usuarios (192.168.1.0/24).

Zona roja (WAN): acceso a Internet simulado (192.168.0.0/24).

Zona naranja (DMZ): servidores públicos (172.16.0.0/24).

La correcta configuración de las tarjetas de red dentro de VirtualBox permitió aislar las zonas y establecer rutas controladas.

6.2 Configuración de NAT

Se implementaron reglas de NAT tipo SNAT desde las zonas verde y naranja hacia la zona roja, garantizando acceso a Internet mediante traducción de direcciones sin exponer las IP privadas. Además, se configuraron reglas de DNAT para reenviar solicitudes desde la WAN hacia servicios en la DMZ.

Estas reglas fueron validadas mediante comandos como ping, curl y navegación desde los clientes.

6.3 Servicios públicos en la zona DMZ

En un servidor Ubuntu Server ubicado en la DMZ, se instalaron los servicios Apache2 y vsftpd, configurados para responder en los puertos estándar 80 (HTTP) y 21 (FTP). Las reglas del firewall de Endian permitieron únicamente tráfico necesario, y se denegaron paquetes ICMP (tipo 8 y 30), restringiendo escaneos de red.

6.4 Reglas de acceso entre zonas

A través de la interfaz de Endian se crearon reglas específicas para permitir el acceso desde la LAN hacia la DMZ y desde la DMZ hacia la WAN, exclusivamente para protocolos HTTP y FTP. También se permitió acceso desde la WAN hacia la DMZ de manera controlada, simulando publicación de servicios.

Las pruebas se realizaron con navegadores web, clientes FTP y revisión de los registros del firewall.

6.5 Proxy HTTP no transparente con autenticación

Se configuró un proxy HTTP no transparente en Endian. Se creó un perfil de filtrado con lista negra para sitios como www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, y se vinculó a una política de acceso basada en autenticación de usuarios internos. La verificación se realizó desde un cliente Ubuntu Desktop en la LAN.

7 TITULO DE PRIMER NIVEL

7.1 ANÁLISIS Y DISCUSIÓN DE RESULTADOS

La ejecución práctica de la arquitectura de seguridad perimetral basada en Endian Firewall permitió validar una solución efectiva y replicable para entornos de red virtualizados. Durante el desarrollo de cada temática, se observaron resultados consistentes con los objetivos propuestos, y se identificaron aspectos clave relacionados con el rendimiento, la aplicabilidad y la administración de la seguridad de red.

En primer lugar, la correcta segmentación de las zonas LAN, WAN y DMZ a través de adaptadores de red virtuales evidenció que la virtualización no representa una limitante para la implementación de entornos reales de seguridad, siempre que se realice una planeación adecuada de IPs y topología.

En relación con las reglas NAT, se comprobó que tanto la traducción de direcciones de salida (SNAT) como la de entrada (DNAT) son mecanismos eficaces para habilitar la conectividad sin comprometer la exposición directa de las IPs internas. Endian facilitó esta configuración con una interfaz gráfica amigable, aunque requiere comprensión previa de conceptos de redes para evitar conflictos de reglas.

La habilitación de servicios en la DMZ (Apache y FTP) reforzó el concepto de zonas desmilitarizadas como perímetros controlados. El filtrado de protocolos como ICMP fue exitoso, lo que demuestra que se puede evitar el reconocimiento de red sin interrumpir los servicios esenciales.

La creación de reglas interzonales de acceso demostró que es posible mantener la funcionalidad sin sacrificar la seguridad, gracias al enfoque de acceso mínimo necesario. Esta política se reflejó claramente en las pruebas realizadas, donde únicamente los protocolos permitidos pudieron establecer comunicación.

Finalmente, la implementación del proxy HTTP no transparente con autenticación de usuarios permitió evidenciar un control fino sobre la navegación. La asociación de listas negras, perfiles y usuarios individuales mostró un modelo de administración robusto, adecuado incluso para entornos institucionales o corporativos.

En general, los resultados obtenidos muestran que es posible construir una infraestructura segura, modular y escalable usando exclusivamente herramientas libres. Esto refuerza la viabilidad del uso de GNU/Linux y soluciones como Endian en proyectos de seguridad perimetral tanto académicos como profesionales.

7.2 TITULO DE TERCER NIVEL

7.3 Configuración De Autenticación En El Proxy

Durante la implementación del proxy HTTP no transparente en Endian Firewall, se procedió a habilitar el módulo de autenticación para controlar el acceso a Internet desde la zona verde (LAN). Este mecanismo permite que únicamente los usuarios registrados puedan navegar, aplicando políticas de seguridad y filtrado personalizadas.

La configuración incluyó los siguientes pasos:

Creación de usuarios: Desde el panel de administración de Endian, se accedió al módulo de proxy y se creó un nuevo usuario con credenciales definidas, el cual fue asociado a un grupo de acceso.

Definición del perfil de filtrado: Se generó un perfil de control de contenido, en el que se estableció una lista negra de dominios web (e.g., www.youtube.com, www.hotmail.com, www.elnuevodia.com.co), los cuales serían bloqueados para todos los usuarios autenticados bajo esa política.

Asociación del perfil a la política de autenticación: Finalmente, el perfil fue vinculado a la política activa de proxy, habilitando el modo de autenticación mediante navegador. Así, al intentar acceder a cualquier sitio web, el usuario debía autenticarse con su nombre de usuario y contraseña para obtener acceso filtrado.

Esta configuración permitió garantizar que solo los usuarios autorizados pudieran utilizar el servicio de navegación, además de registrar los intentos de acceso bloqueados mediante los logs del sistema, proporcionando trazabilidad de uso.

8 Conclusiones.

La implementación de un entorno seguro mediante **Endian Firewall Community** en una infraestructura virtualizada permitió consolidar los conceptos y prácticas fundamentales de la seguridad perimetral en redes GNU/Linux. A través del desarrollo de cinco temáticas clave, se diseñó una arquitectura de red segmentada, funcional y replicable, que reproduce escenarios reales de protección y control de tráfico.

La primera fase del proyecto evidenció la importancia de una **configuración inicial precisa** en VirtualBox, donde la correcta asignación de adaptadores de red y direcciones IP facilitó la segmentación lógica entre la LAN (zona verde), DMZ (zona naranja) e Internet simulada (zona roja). Esta estructura fue fundamental para aplicar políticas de acceso diferenciales.

Posteriormente, la configuración de reglas de **NAT (Network Address Translation)** permitió el acceso seguro desde las redes internas hacia el exterior, ocultando las direcciones privadas y mejorando la seguridad del entorno. Esta funcionalidad, fácilmente administrable desde Endian, demostró ser crucial para mantener conectividad sin comprometer la privacidad de la topología interna.

La exposición controlada de servicios públicos en la zona **DMZ**, como HTTP y FTP, se combinó con el bloqueo del protocolo ICMP, permitiendo ofrecer servicios esenciales sin riesgos asociados al reconocimiento de red. Este enfoque evidenció el valor de limitar el tráfico a los protocolos necesarios, fortaleciendo la defensa en profundidad.

La definición de **reglas de acceso interzonales** proporcionó un control granular del tráfico, aplicando el principio de mínimo privilegio. Se permitió exclusivamente el tránsito entre zonas requerido para la operación de los servicios, lo cual se validó con pruebas funcionales y análisis de logs.

Finalmente, la integración de un **proxy HTTP no transparente con autenticación de usuarios** permitió filtrar contenidos, registrar accesos y aplicar políticas individualizadas de navegación. Este mecanismo reforzó la trazabilidad y el control sobre el tráfico web desde la red interna, mostrando el potencial de Endian como solución integral de seguridad.

En conjunto, la actividad desarrollada no solo facilitó la comprensión y aplicación de herramientas de código abierto en la protección de redes, sino que también fortaleció competencias en virtualización, administración de servicios, segmentación de red, reglas de firewall, NAT y gestión de contenidos. Se concluye que una solución bien planificada y correctamente implementada como la aquí descrita puede ser una alternativa viable, segura y escalable para entornos académicos, institucionales y empresariales.

8.1 CITAS Y/O REFERENCIAS

[1] Endian, Endian UTM 3.2 - Manual de referencia, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[2] Canonical, Guía del Ubuntu Desktop 20.04 LTS, Ubuntu Help, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Linux Professional Institute, “Linux Essentials – Tema 102: Comandos GNU y Unix”, 2023. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[4] Oracle, Manual de usuario de VirtualBox, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[5] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server, 3ra ed., Packt Publishing, 2020.

8.2 REFERENCIAS

[1] Endian, Endian UTM 3.2 - Manual de referencia, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[2] Canonical, Guía del Ubuntu Desktop 20.04 LTS, Ubuntu Help, 2023. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Linux Professional Institute, “Linux Essentials – Tema 102: Comandos GNU y Unix”, 2023. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[4] Oracle, VirtualBox User Manual, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[5] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server, 3ra ed., Packt Publishing, 2020.

[6] Debian Project, Manual del administrador de Debian 12.5.0, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[7] Universidad Nacional Abierta y a Distancia (UNAD), Guía de aprendizaje – Etapa 7: Implementando seguridad en GNU/Linux, Escuela de Ciencias Básicas, Tecnología e Ingeniería, 2025.